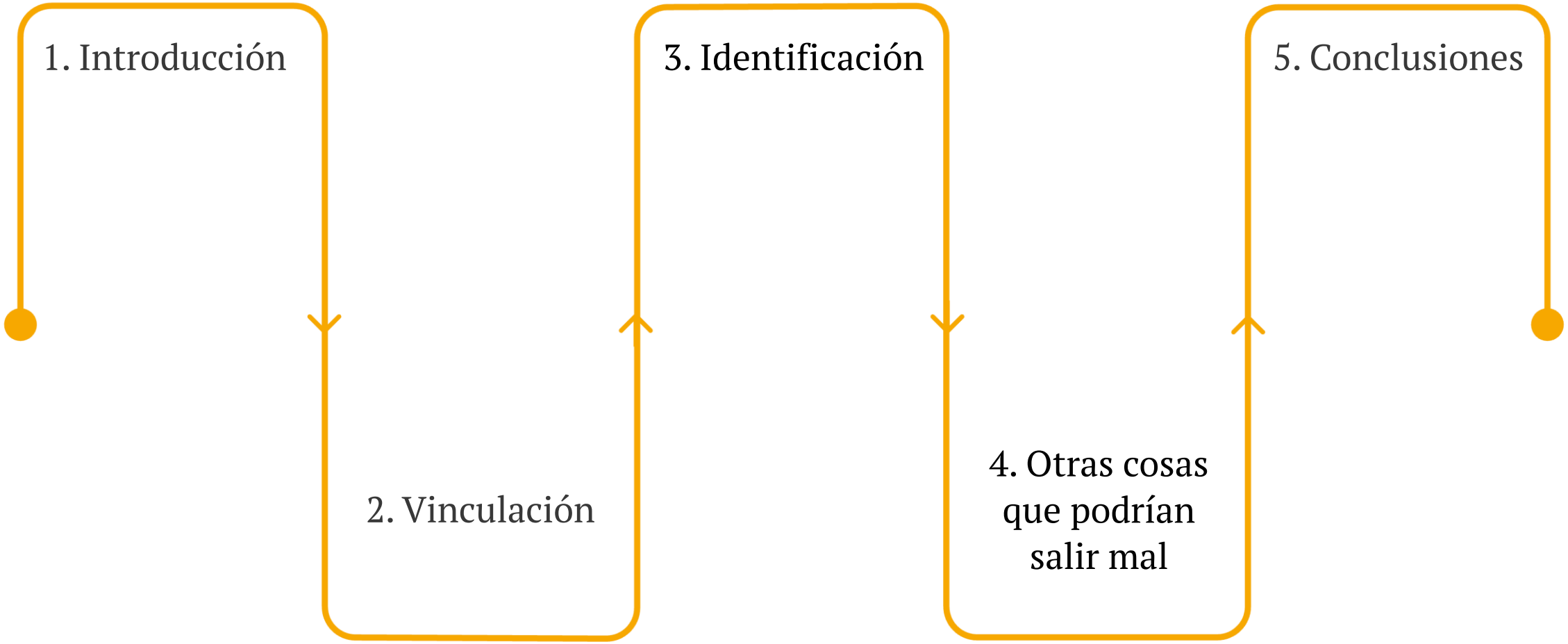
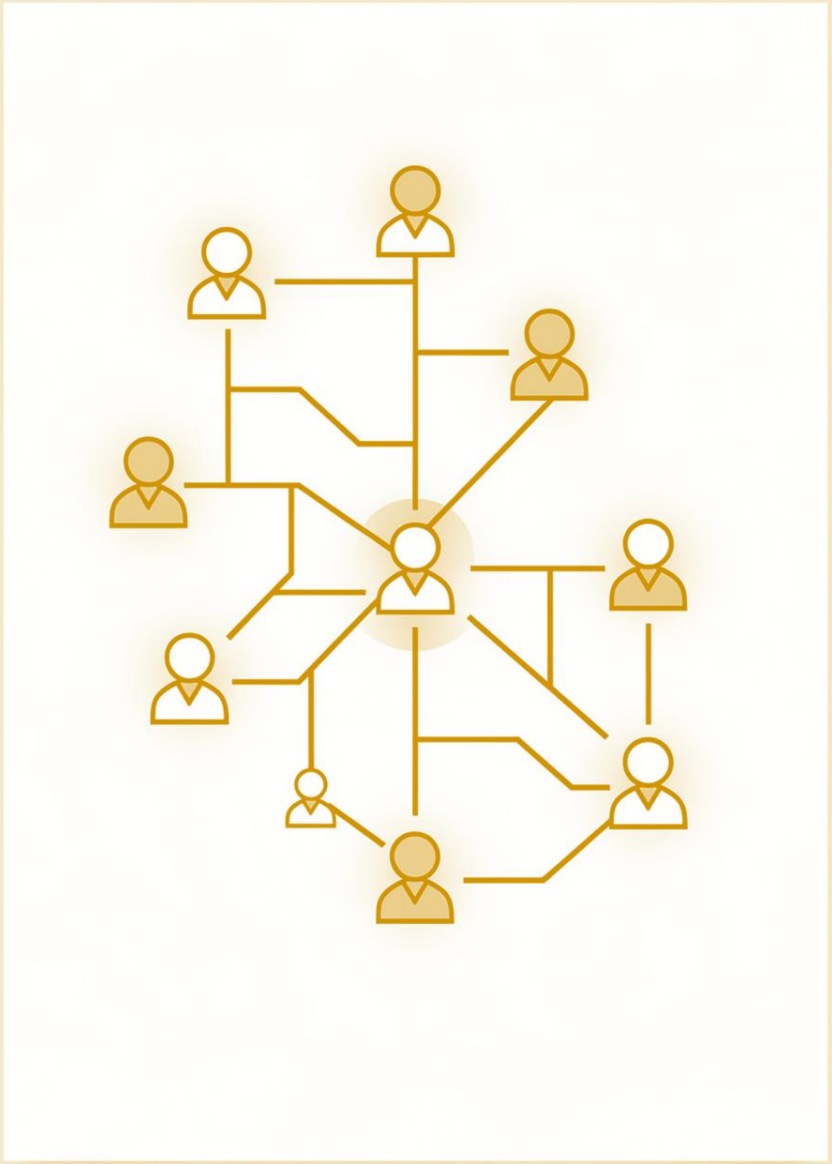
La nueva cartera de identidad digital europea: ¿poder para los usuarios o puerta a la vigilancia masiva?

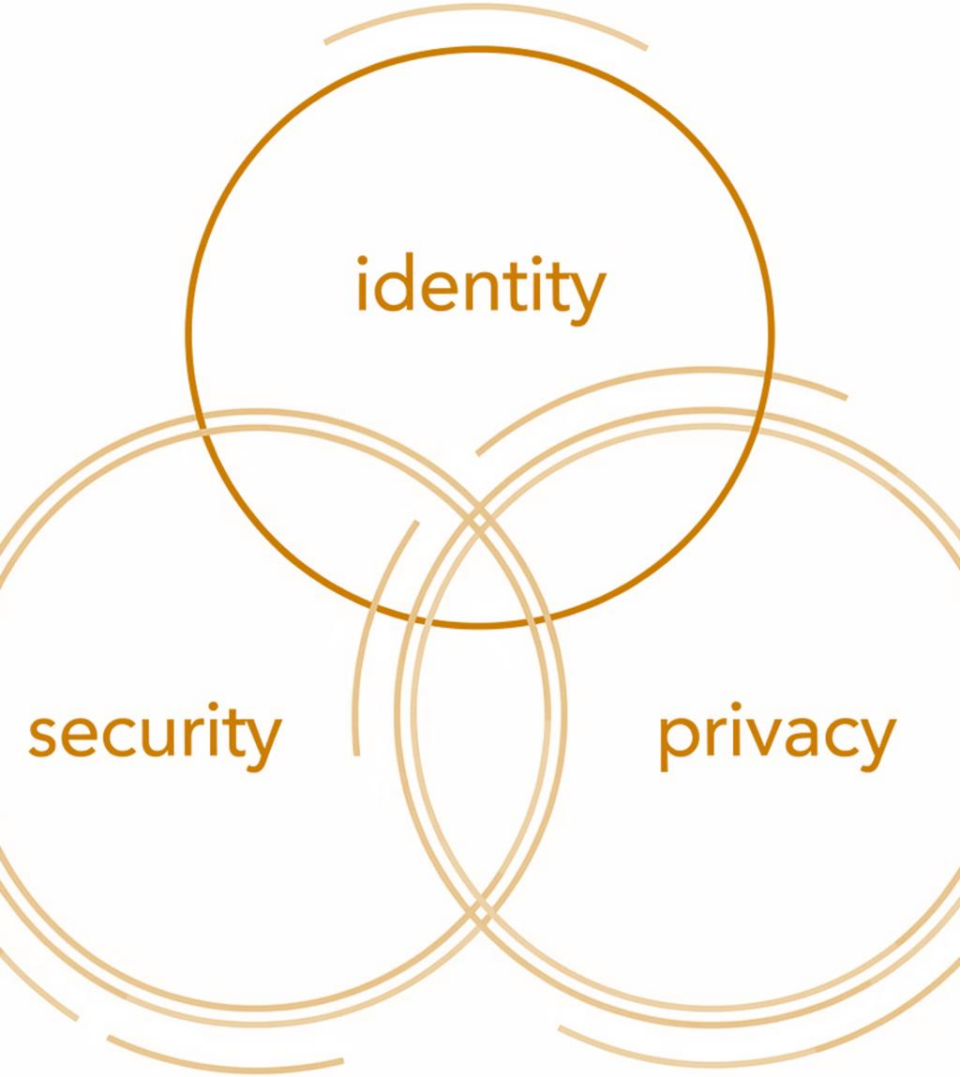
MARTA BELTRÁN

Contenidos


1. Introducción
2. Vinculación
3. Identificación
4. Otras cosas que podrían salir mal
5. Conclusiones



1. Introducción



Un triángulo inseparable

Identidad

Quién eres y cómo lo demuestras ante sistemas, servicios digitales y terceros.

Seguridad

Cómo se protegen la confidencialidad, la integridad y la disponibilidad de tus activos.

Privacidad

El derecho a controlar qué se sabe de ti, quién lo sabe y para qué.

Las preguntas que debemos hacernos desde el punto de vista de protección de datos

Sobre los datos

¿Qué datos se recogen para gestionar la identidad? ¿Cómo se obtienen? ¿Por qué esos datos y no otros? ¿Qué condiciones rigen su uso?

Sobre los participantes

¿Quién participa en la gestión de la identidad? ¿Qué papel tiene cada actor y a qué datos accede? ¿Cual es el modelo de confianza?

Sobre el ejercicio de derechos

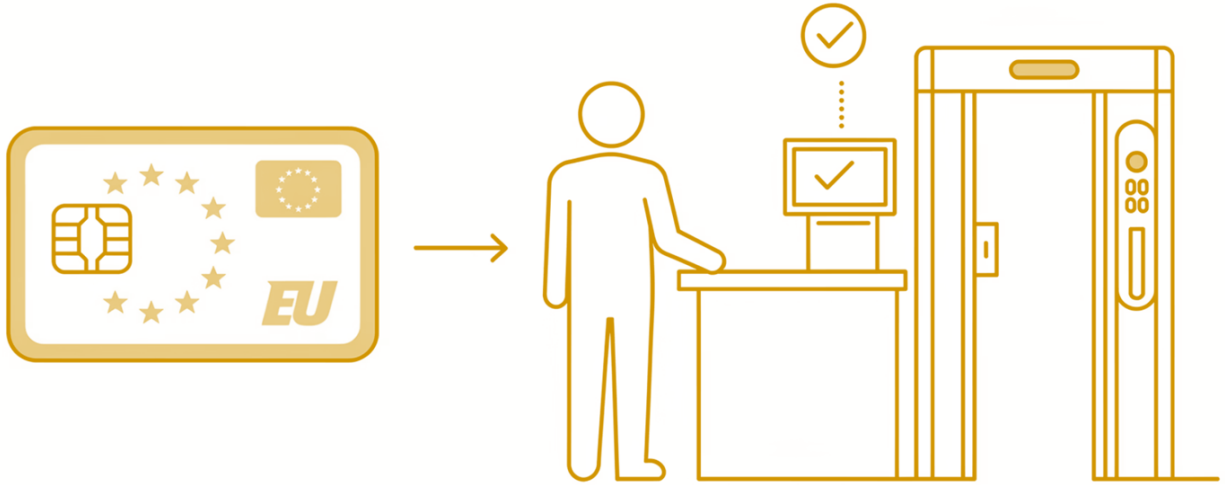
¿Han sido informados los usuarios de forma clara y comprensible sobre todos los aspectos anteriores? ¿Pueden objetar?

La identidad como derecho fundamental

> La gestión de la identidad no es un servicio tecnológico más. De ella depende nuestra capacidad para obrar como ciudadanos y el ejercicio de múltiples derechos fundamentales y libertades.

Gestionarla como mera infraestructura técnica supone ignorar su dimensión constitucional. Debe reconocerse, regularse, diseñarse e implementarse como un derecho.

https://www.aepd.es/prensa-y-comunicacion/blog/la-identidad-como-derecho



REGLAMENTO EIDAS

El primer marco europeo de identidad digital

eIDAS garantiza que ciudadanos y empresas puedan utilizar sus sistemas nacionales de identificación electrónica (eID) para acceder a servicios públicos en cualquier Estado miembro de la UE.

Su objetivo: un mercado interior europeo para los servicios de confianza, con plena validez legal transfronteriza.

¿Qué permite el eIDAS en la práctica?

Declaraciones fiscales

Presentación de impuestos en otro Estado miembro sin desplazamiento.

Universidades extranjeras

Inscripción en centros educativos europeos de forma remota y verificada.

Cuentas bancarias

Apertura remota de cuentas con plena validez legal en cualquier banco europeo.

Creación de empresas

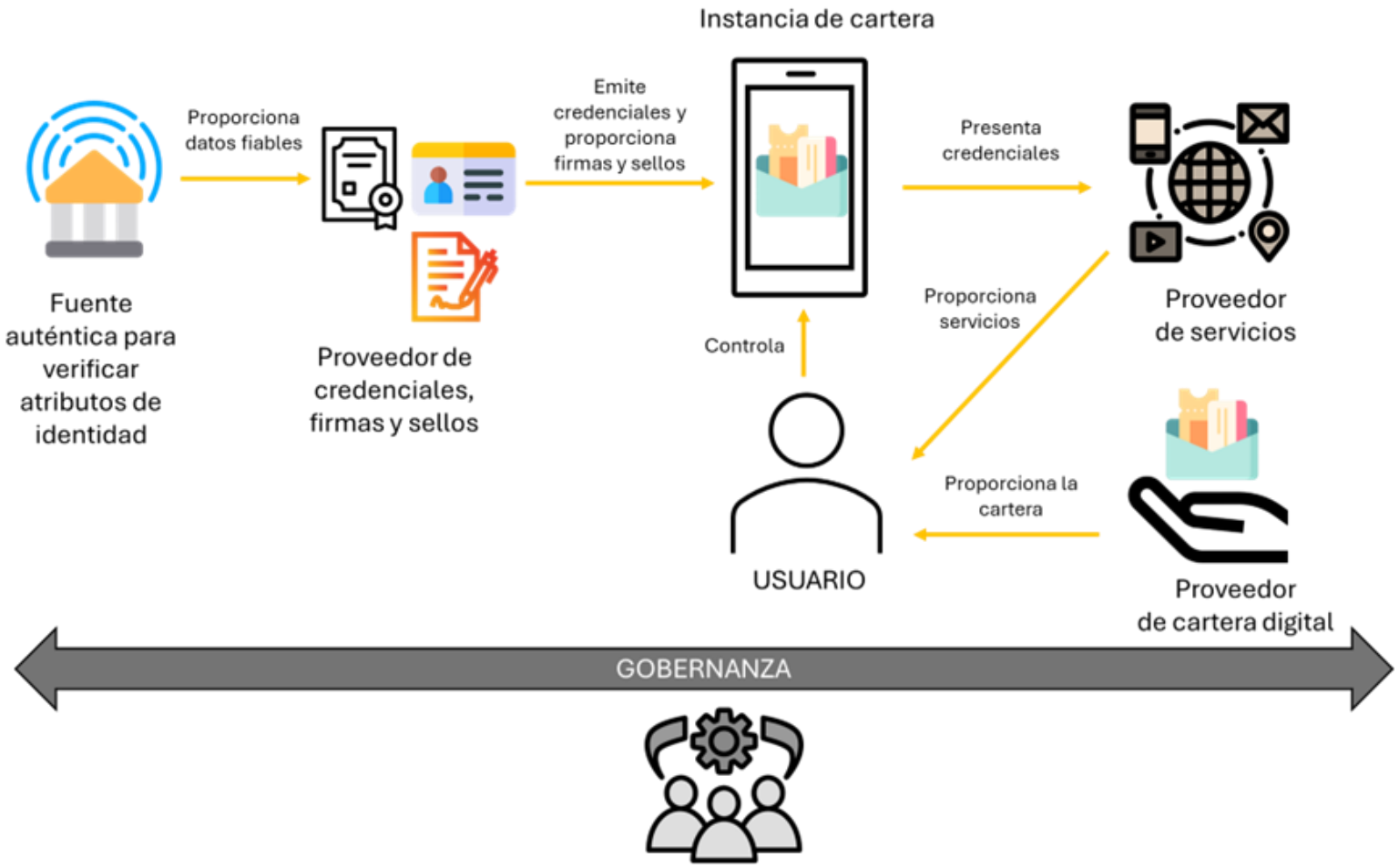
Alta de sociedades en otros Estados miembros sin presencia física.

2021 · PROPUESTA DE LA COMISIÓN EUROPEA

La evolución necesaria: eIDAS2

El diagnóstico fue claro: escasa penetración del eIDAS original. En 2021, la Comisión Europea publicó una propuesta revisada para corregir sus carencias y ampliar su alcance.

Modelo descentralizado



https://www.aepd.es/prensa-y-comunicacion/blog/eldas2-la-cartera-europea-de-identidad-digital-y-el-rgpd-i

REGLAMENTO (UE) 2024/1183 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 11 de abril de 2024 por el que se modifica el Reglamento (UE) n.o 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (eIDAS2)

Regulación y especificaciones técnicas

- Commission Implementing Regulation (CIR)
- ARF
- Certification scheme

Implementaciones y ecosistema

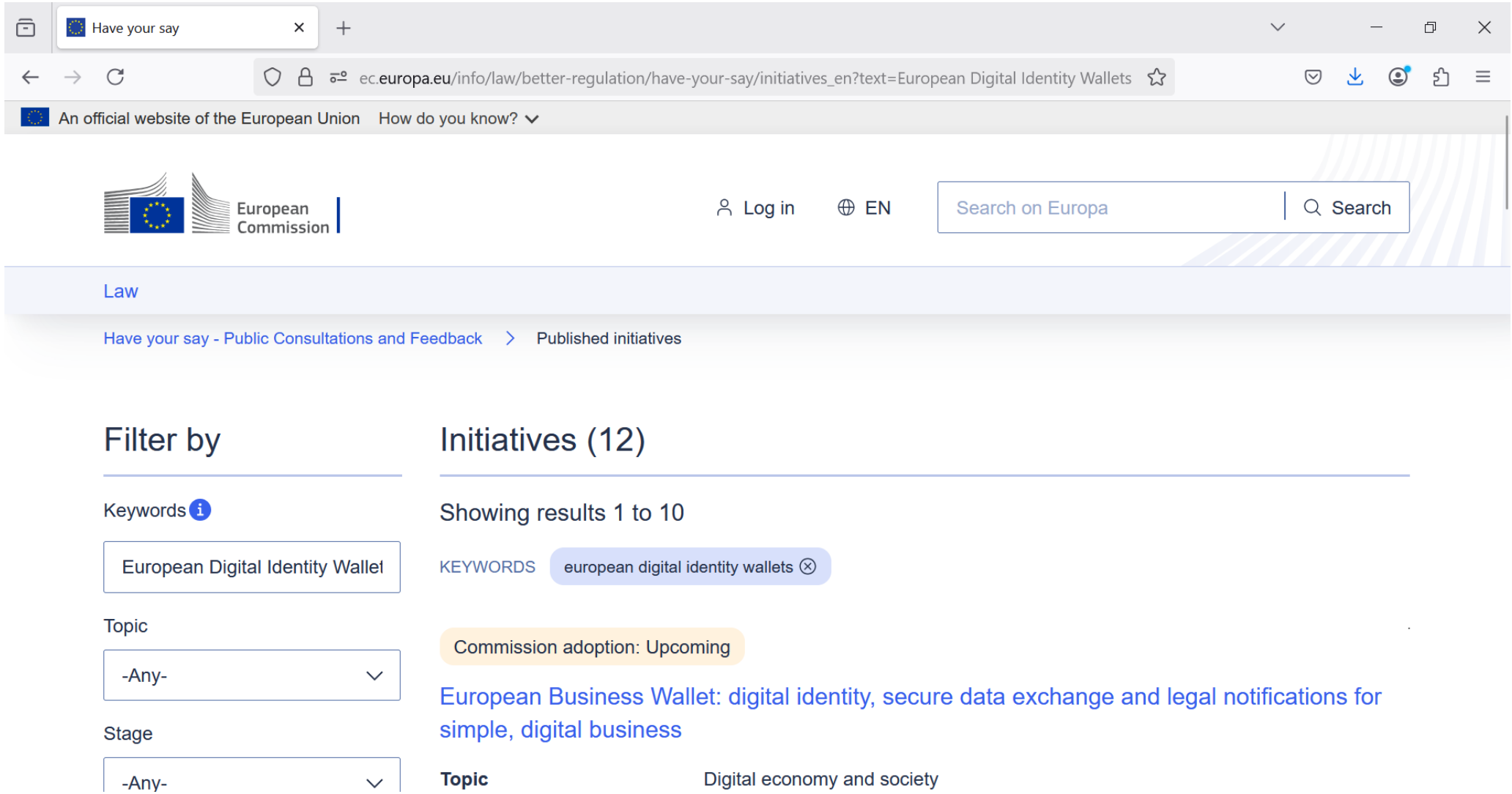
- Estados Miembros
- Proveedores de cartera
- Proveedores de credenciales, firmas, etc.

Gobernanza y supervisión

- CABs
- Autoridades nacionales de certificación y acreditación
- Autoridades de Protección de Datos

Validación, pruebas, consultas públicas, grupos de trabajo

El papel de la AEPD: Implementing Acts



El papel de la AEPD: Implementing Acts

Innovation and technology division
1 / 2

Spanish Data Protection Authority
AEPD, Agencia Española de Protección de Datos
Calle Jorge Juan, 6. 28001 Madrid, Spain
https://www.aepd.es/
División de Innovación Tecnológica
dit@aepd.es

Feedback on the Commission Implementing Regulation (EU) .../... Of xxx laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards qualified electronic attestations of attributes and electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source:

The provided draft Implementing Act already includes several provisions to align with the GDPR. However, there are potential areas for improvement to strengthen data protection further:

- Emphasize data minimization: Although the draft mandates the inclusion of only essential information in attribute catalogues, further reinforcement of data minimization is possible. This could involve establishing clear criteria for determining the necessity of attributes to be included in the catalogue or exploring mechanisms to limit the scope of data collected for each attribute. For example, granular consent options should be implemented to allow individuals to choose which specific attributes they want to share/use to issue attestations.
- Address specific concerns regarding revocation: The draft mandates revocation mechanisms but does not provide practical guidance on the procedures and timeframes for revocation or address the potential challenges of revoking

Innovation a

Spanish Data Protection Authority
AEPD, Agencia Española de Protección de Datos
Calle Jorge Juan, 6. 28001 Madrid, Spain
https://www.aepd.es/
División de Innovación Tecnológica
dit@aepd.es

Feedback on the Commission Implementing Regulation (EU) ..
down rules for the application of Regulation (EU) No
EuropeanParliament and of the Council as regards reactions to se
European Digital Identity Wallets:

The provided draft Implementing Act already includes several provisi
GDPR. However, there are potential areas for improvement to strengt
further:

- Define reliability: Since the "reliability" property is not definec
clear whether it includes the traditional security triad attribu
integrity, availability) or includes other aspects related to tr
as the ability to fulfil the specified requirements for which it

Innovation and technology division
1 / 2

Spanish Data Protection Authority
AEPD, Agencia Española de Protección de Datos
Calle Jorge Juan, 6. 28001 Madrid, Spain
https://www.aepd.es/
División de Innovación Tecnológica
dit@aepd.es

Feedback on the Commission Implementing Regulation (EU) .../... Of xxx laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards cross-border identity matching of natural persons by public sector bodies

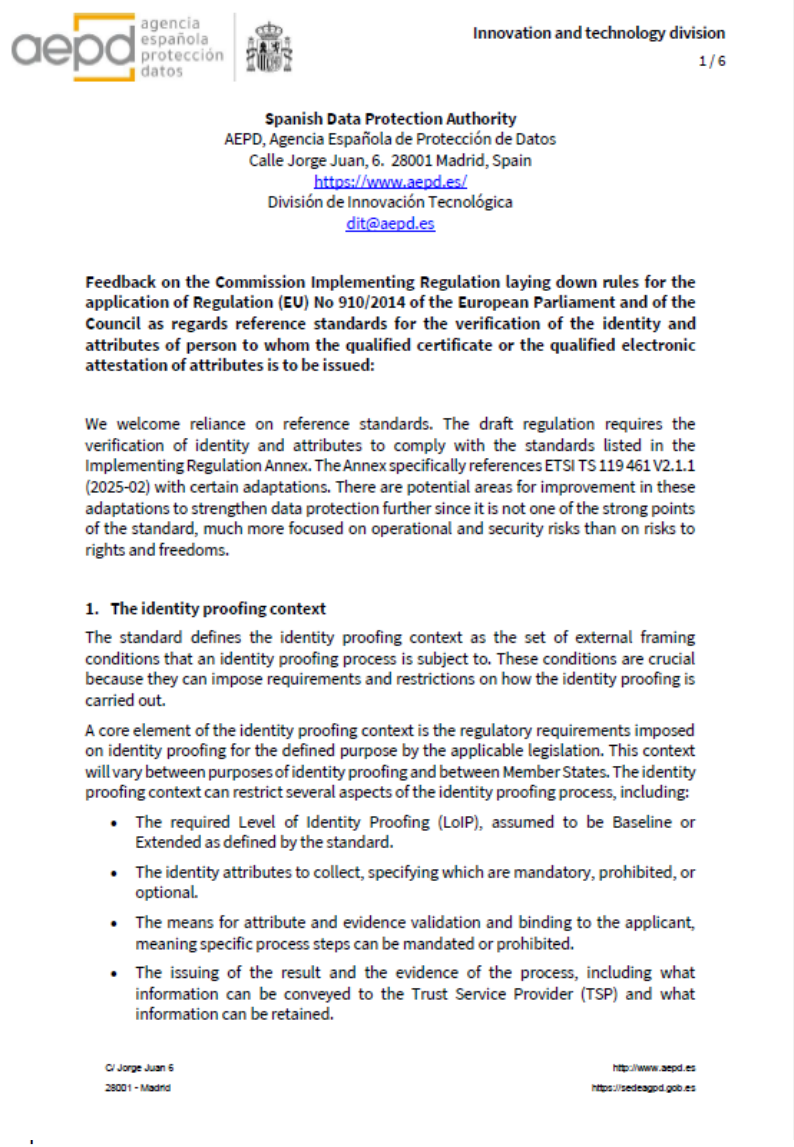
The draft outlines a process for "unequivocal identity matching" that requires relying parties to obtain, validate, and match specific attributes from users against existing records. This process necessarily involves the processing of personal data, and the draft emphasises the need for a successful match for precisely one natural person to minimise

Innovation a

Spanish Data Protection Authority
AEPD, Agencia Española de Protección de Datos
Calle Jorge Juan, 6. 28001 Madrid, Spain
https://www.aepd.es/
División de Innovación Tecnológica
dit@aepd.es

Feedback on the Commission Implementing Regulation (EU) ...
down rules for the application of Regulation (EU) No 910/2014
Parliament and of the Council as regards the registration of wall
and the common mechanism for the identification and authent
relying parties:

The EUDI Wallet will be used in very different use cases: sor
identification/authentication (for example, borders or payment), while others require anonymity (for example, age verification). These situations should lead to over-identification, allowing all RPs in all use cases to identify/authenticate data subjects.



Innovation and technology division
1 / 6

Spanish Data Protection Authority
AEPD, Agencia Española de Protección de Datos
Calle Jorge Juan, 6. 28001 Madrid, Spain
https://www.aepd.es/
División de Innovación Tecnológica
dit@aepd.es

Feedback on the Commission Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for the verification of the identity and attributes of person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued:

We welcome reliance on reference standards. The draft regulation requires the verification of identity and attributes to comply with the standards listed in the Implementing Regulation Annex. The Annex specifically references ETSI TS 119 461 V2.1.1 (2025-02) with certain adaptations. There are potential areas for improvement in these adaptations to strengthen data protection further since it is not one of the strong points of the standard, much more focused on operational and security risks than on risks to rights and freedoms.

1. The identity proofing context

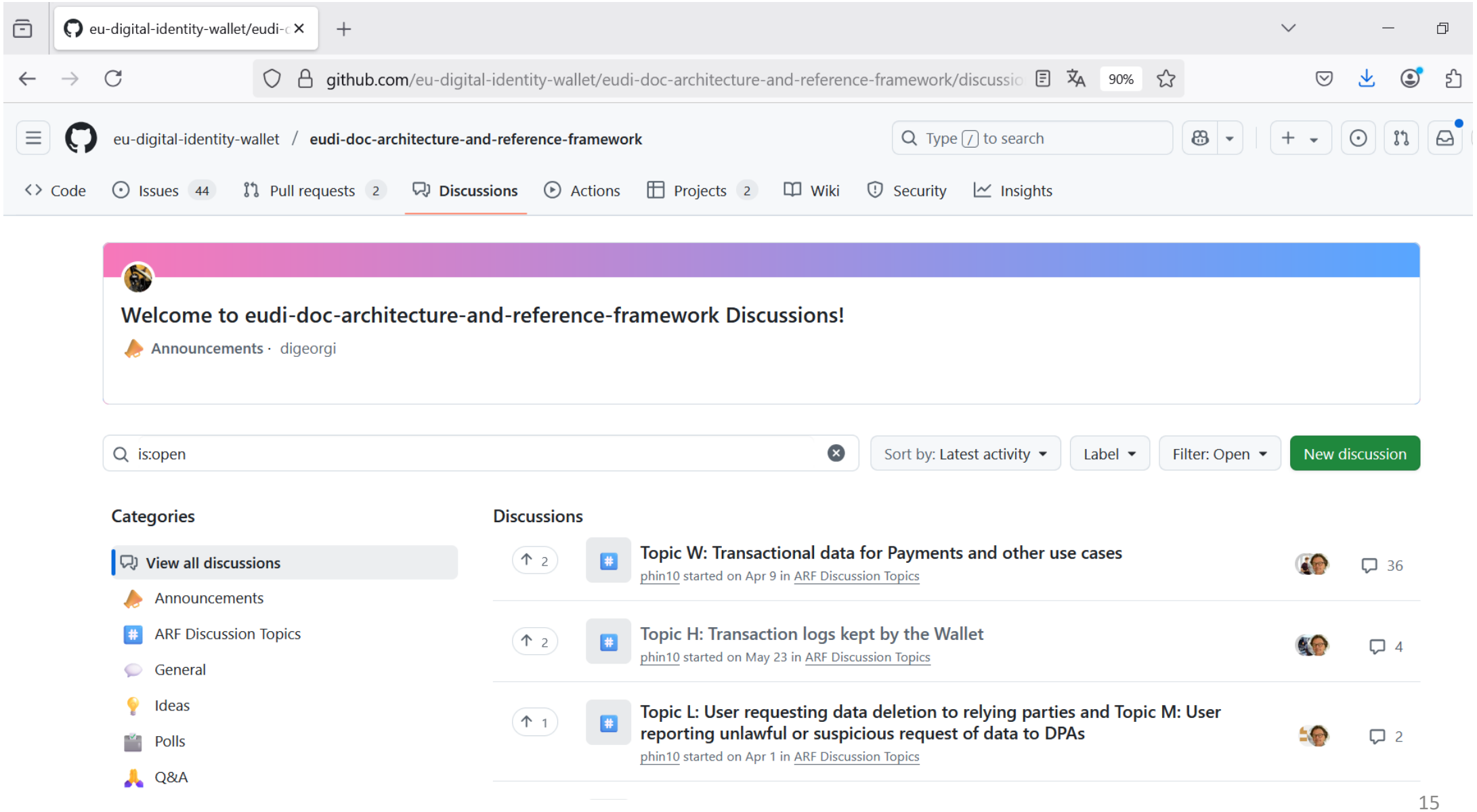
The standard defines the identity proofing context as the set of external framing conditions that an identity proofing process is subject to. These conditions are crucial because they can impose requirements and restrictions on how the identity proofing is carried out.

A core element of the identity proofing context is the regulatory requirements imposed on identity proofing for the defined purpose by the applicable legislation. This context will vary between purposes of identity proofing and between Member States. The identity proofing context can restrict several aspects of the identity proofing process, including:

- The required Level of Identity Proofing (LoIP), assumed to be Baseline or Extended as defined by the standard.
- The identity attributes to collect, specifying which are mandatory, prohibited, or optional.
- The means for attribute and evidence validation and binding to the applicant, meaning specific process steps can be mandated or prohibited.
- The issuing of the result and the evidence of the process, including what information can be conveyed to the Trust Service Provider (TSP) and what information can be retained.

C/ Jorge Juan 6
28001 - Madrid
http://www.aepd.es
https://sedeagpd.gob.es

El papel de la AEPD: ARF



El papel de la AEPD: ARF

Topic	Title	
A	Privacy risks and mitigation	Roadmap issue
B	Re-issuance and batch issuance of PIDs and Attestations	Roadm
C	Wallet Unit Attestation (WUA) and Key Attestation	Roadm
D	Embedded Disclosure Policies	Roadm
E	Pseudonyms, including User authentication mechanism	Roadm
F	Digital Credentials API	Roadm
G	Zero Knowledge Proof	Roadm
V	PID Rulebook	Roadm
X	Relying Party registration	Roadm

Topic	Title	
H	Transaction logs kept by the wallet	Roadmap issue
I	Natural person representing another natural person	Roadmap issue
J	Wallet to Wallet interaction	Roadmap issue
K	Combined presentation of Attestations	Roadmap issue
L	User requesting data deletion to Relying Parties	Roadmap issue
M	User reporting unlawful or suspicious request of data to DPAs	Roadmap issue
N	Data portability	Roadmap issue
U	EUDI Wallet Trust Mark	Roadmap issue
W	Transactional data for payments and other use cases	Roadmap issue

Topic H: Transaction logs kept by the Wallet #537

phin10 on May 23 · 2 comments · 2 replies

AEPDmbeltran 2 weeks ago

Comentario original en inglés - Traducir al español

On behalf of the Spanish Data Protection Authority (AEPD)

The attached document contains our comments on this topic.

topicH AEPD response.pdf

Thank you very much for this opportunity to contribute to this important discussion.

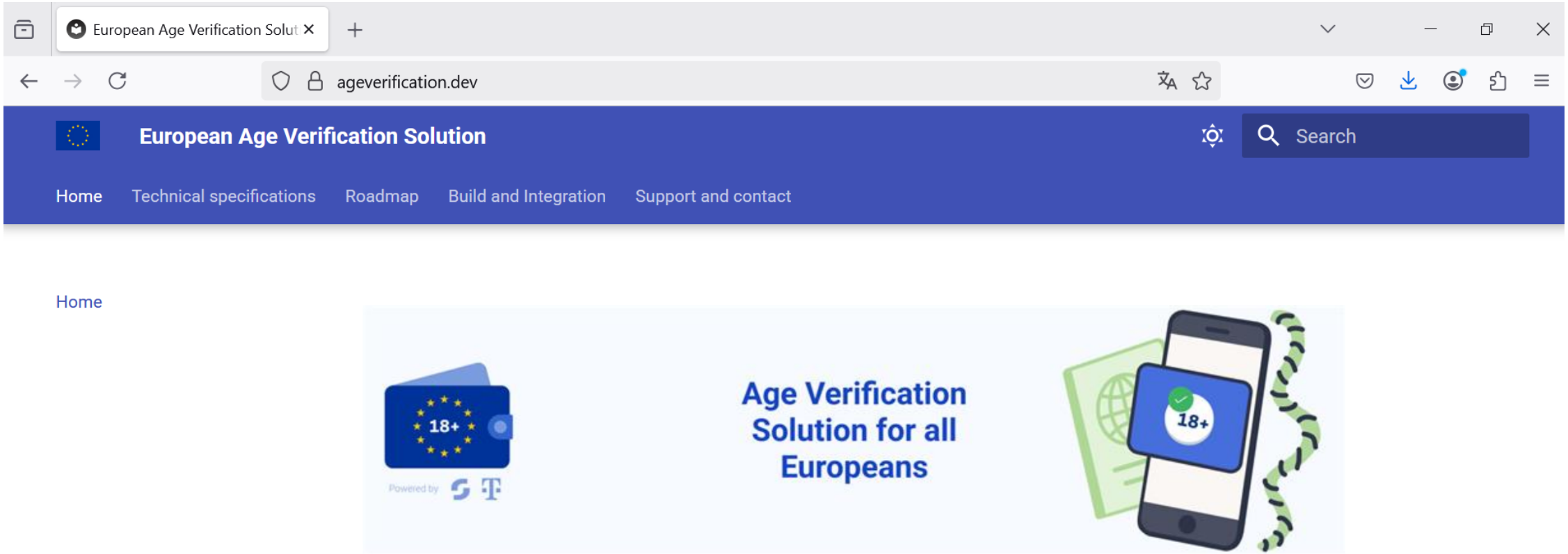
↑ 1 ☺ 1 reply

tmielnicki last week edited

Comentario original en inglés - Traducir al español

> **On behalf of the Spanish Data Protection Authority (AEPD)**
>
> The attached document contains our comments on this topic.
>
> topicH AEPD response.pdf
>
> Thank you very much for this opportunity to contribute to this important discussion.

Thank you for your document, we are analysing it and will provide the response once ready.


European Age Verification Solut
ageverification.dev
European Age Verification Solution
Search
Home
Technical specifications
Roadmap
Build and Integration
Support and contact
Home
18+
Powered by
Age Verification Solution for all Europeans
18+
EU Age Verification Solution
The European Commission is defining a common EU-wide approach to age verification and delivering a white label solution to support its practical adoption across Member States.
This privacy-preserving solution allows users to prove they are old enough to access age-restricted online services, without disclosing unnecessary personal information. It is built on the European Digital Identity Wallet framework and supports compliance

El papel del EDPB

Agenda

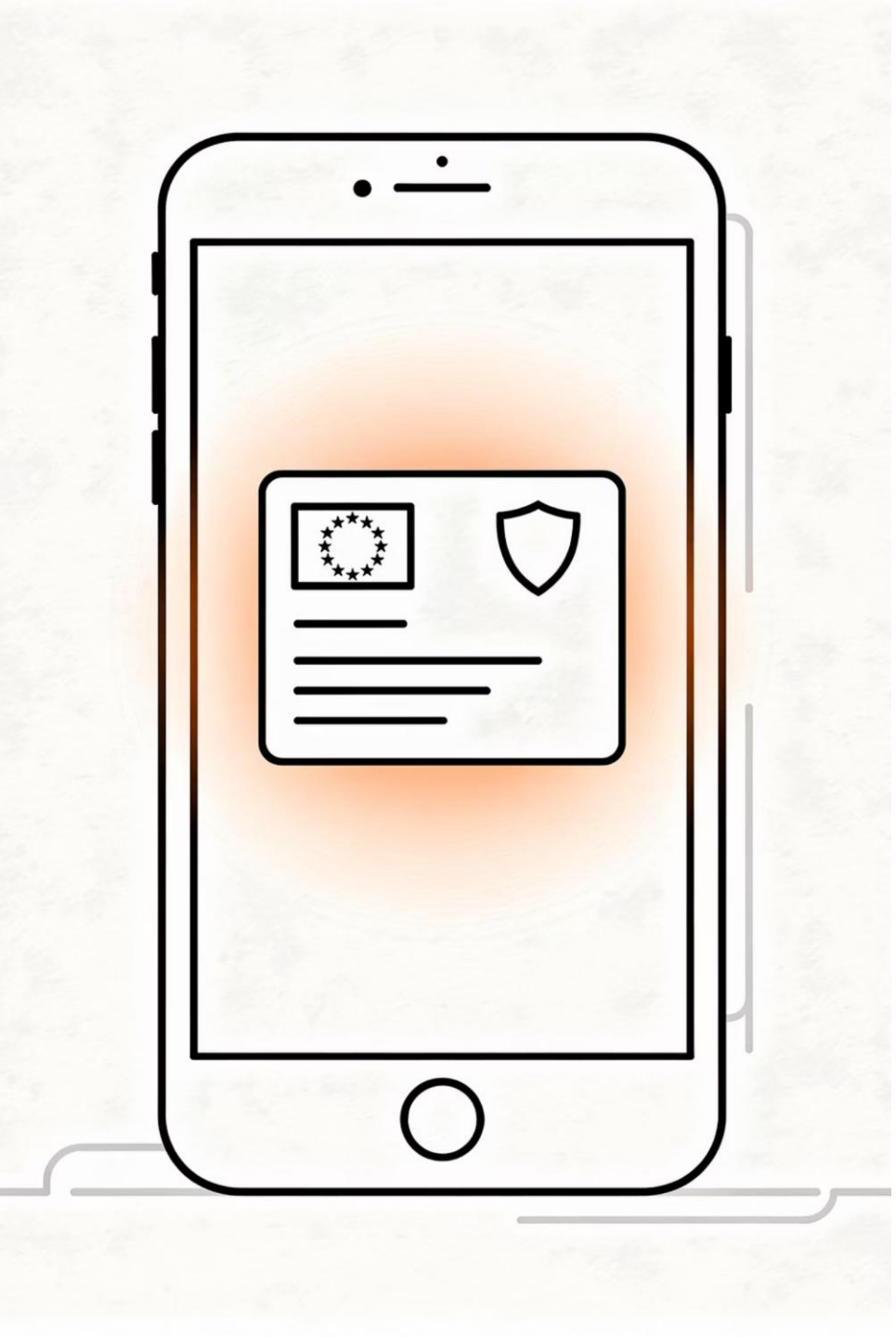
106th EDPB meeting

3 June 2025

Brussels

C. Organisational matters

C.1. Appointment of EDPB representative(s) as observer(s) at the European Digital Identity Cooperation Group (EDICG) and the working group of EDICG under the electronic IDentification, Authentication and Trust Services (eiDAS) cooperation group



2. Vinculación

La cartera estará presente en diferentes casos de uso

🛂 Identificación completa y autenticación

Paso de fronteras, servicios financieros (KYC), registro en servicios regulados. Requieren autenticación segura del usuario.

🔒 Compartición de atributos y autorización

Verificación de edad, beneficios para familias numerosas o por nacionalidad, tarjeta de aparcamiento para discapacitados. Deben preservar el anonimato del usuario.

¿Qué es la amenaza de Vinculación?

La vinculación permite asociar la actividad digital de un ciudadano, sus diferentes sesiones o transacciones, para realizar seguimiento o crear perfiles, por ejemplo.

Rastreo

Seguimiento de actividad digital.

Perfilado

Evaluación de aspectos personales para analizar o predecir preferencias, hábitos, etc.

¿Qué se debe garantizar?

Tres garantías esenciales:

Inobservabilidad frente al emisor

Los emisores no deben rastrear el uso de credenciales (cuándo, dónde, con quién).

No vinculación multi-presentación

Cada uso de una credencial debe ser indistinguible de los demás, incluso para el mismo proveedor.

No vinculación total

Ningún actor del ecosistema (emisores, proveedores de carteras, RPs) deben poder rastrear la actividad del ciudadano, individualmente o colaborando entre ellos.

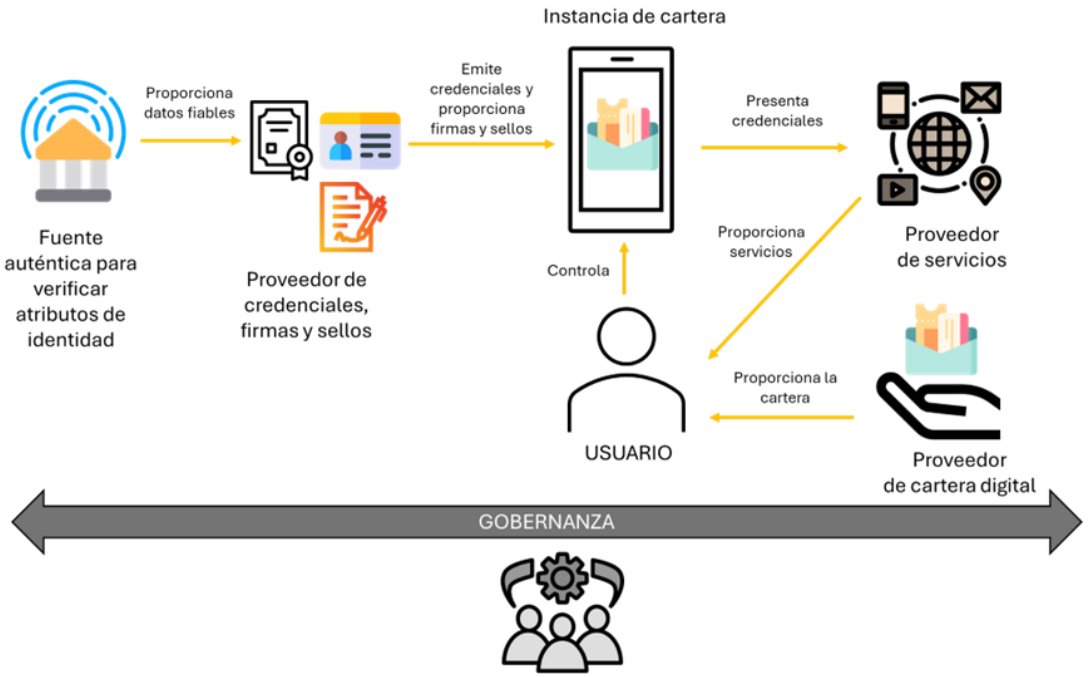
Importante: eIDAS2 sienta las bases legales correctas. El desafío es que las CIR y el ARF traduzcan la obligación de “no vinculación” en requisitos técnicos vinculantes y una realidad, no solo una aspiración.

Pregunta 1: Inobservabilidad
¿Puede saber el emisor de credenciales dónde las uso?

Materialización de la amenaza

Si el emisor almacena identificadores únicos o pseudo-identificadores y un proveedor (RP) los comparte (ej. para realizar comprobaciones, para facturar), el emisor podría rastrear el uso de las credenciales que ha realizado el ciudadano.

Cuando hay peticiones síncronas de credenciales, el emisor puede saber, cómo mínimo, cuándo se están utilizando.



Pregunta 2: No vinculación multi-presentación ¿Pueden los servicios vincular mis accesos anónimos?

Misma RP

Identificadores, pseudo-identificadores, metadatos u otros datos no revelados explícitamente pueden permitir a una RP vincular múltiples transacciones del mismo ciudadano anónimo en distintas sesiones o transacciones.

Entre diferentes RPs

El potencial de rastreo o perfilado aumenta si distintas RP colaboran para vincular transacciones de un mismo ciudadano que usa la misma credencial o diferentes credenciales que comparten identificadores, pseudo-identificadores, etc.

Impacto

Perfiles detallados (targeting, micro-targeting, addressability), precios diferenciados, soporte para la amenaza de Identificación.

Pregunta 3: No vinculación total ¿Y si se combina información?

Materialización de la amenaza

Cooperación entre partes

La colaboración entre emisores de credenciales y RPs permite vincular transacciones y crear perfiles de usuario detallados.

Brecha de datos combinada

Una brecha de datos en emisor y/o RPs puede permitir a terceros cruzar información y construir perfiles de usuario.

Propiedad importante: Full Unlinkability

El problema técnico: firmas como identificadores

Firmas criptográficas: un identificador persistente

Los formatos de credencial soportados, ISO mDL y SD-JWT, usan firmas criptográficas para la validación. Estas firmas actúan como identificadores únicos y persistentes, permitiendo reconocer que dos presentaciones distintas provienen del mismo titular, incluso si los atributos revelados son diferentes.

Importante: Una credencial firmada es rastreable en múltiples sesiones o transacciones, no garantiza la no vinculación. La única opción es utilizar credenciales de corta duración y un único uso (usar y tirar) pero no es para nada una solución perfecta.

Firma = ID único

Cada credencial lleva una firma que la identifica de forma única.

Vinculación de sesiones

Múltiples presentaciones con la misma firma son correlacionables.

Metadatos adicionales

Otros identificadores (IP, marcas de tiempo) agravan el problema.

Otro problema: los mecanismos de revocación

1

RP consulta al emisor

Cuando la RP verifica la validez con el emisor, este sabe cuándo y dónde el ciudadano usa su credencial.

2

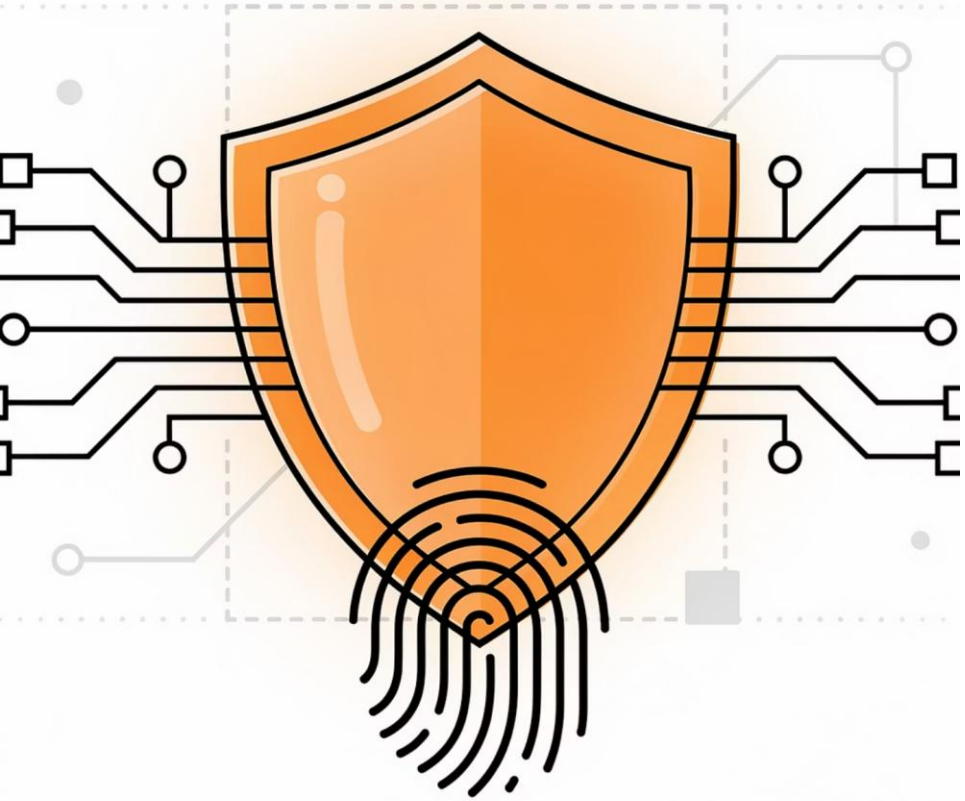
Correlación de marcas de tiempo

La RP puede correlacionar presentaciones del mismo usuario por el estado de revocación o las marcas de tiempo, incluso con atributos diferentes.

3

Rastro de actividad

Cada verificación de revocación genera un registro que el emisor puede usar para reconstruir el patrón de actividad del ciudadano.



3. Identificación

¿Qué es la amenaza de Identificación?

La amenaza de identificación surge cuando emisores de credenciales, Relying Parties (RP) o proveedores de carteras conocen de forma inapropiada o innecesaria la identidad real de un usuario. La amenaza de Divulgación está muy relacionada, cuando no se cumple el principio de minimización de datos.

Importante: Un ciudadano debe poder demostrar que es mayor de edad, estudiante o miembro de una asociación sin revelar su identidad completa.

¿Qué se debe garantizar?

Registro y transparencia de RPs

Las RPs deben declarar qué datos necesitan para cada caso de uso. La cartera alerta al ciudadano ante cualquier desviación, por ejemplo, que solicita identificación cuando no es necesaria.

Seudónimos locales por RP

Los seudónimos únicos por Relying Party son la primera línea de defensa contra la sobre-identificación y, además evitan la correlación entre transacciones en diferentes RP.

Revelación selectiva + no vinculación

La revelación selectiva, que permite seleccionar los atributos que se presentan, es necesaria pero no suficiente. También es importante que no se pueda materializar la amenaza de Vinculación

Importante: De nuevo eIDAS2 incorpora principios y requisitos que van en la buena dirección, pero hay que garantizar que el diseño y la implementación de las futuras carteras cumplen estas obligaciones realmente.

Pregunta 1: Caso directo
¿Y si una RP solicita más datos de los necesarios?

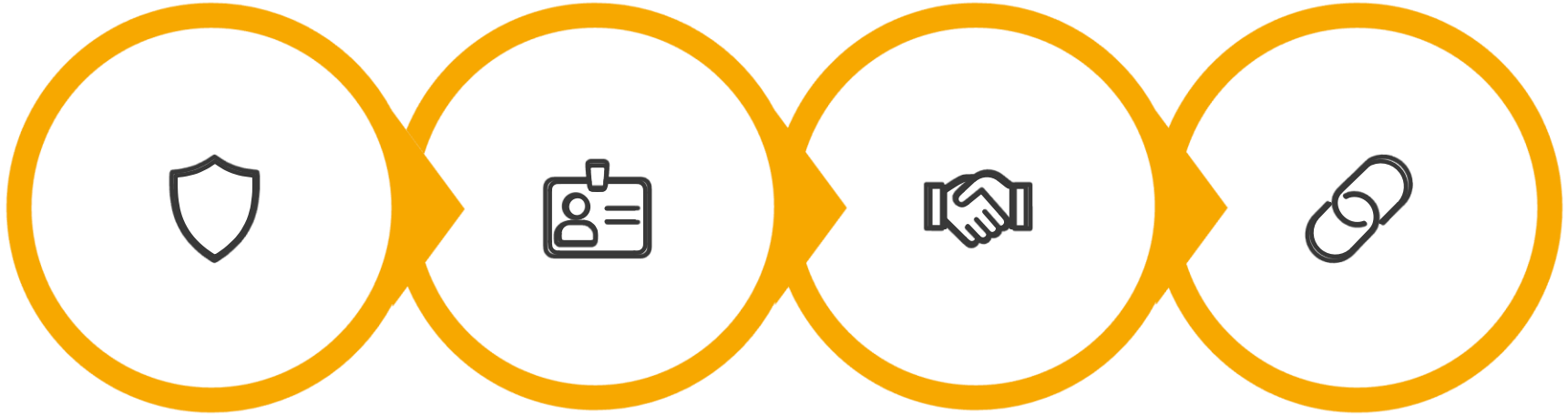
Registro obligatorio de RPs

Las RP deben registrarse en su Estado miembro especificando exactamente qué datos solicitarán y con qué finalidad. No pueden solicitar nada adicional.

Transparencia pública

La información de registro de las RP es accesible públicamente. La cartera alerta al usuario si se solicita información no prevista y le permite rechazar la transacción. También comunicarlo a la autoridad de protección de datos.

Pregunta 2: Caso indirecto
Pero ¿no me protege la revelación selectiva?



Presentación selectiva

Combinación de casos de uso

Colusión de actores

Correlación por emisor

La revelación selectiva por sí sola no evita la Identificación si los elementos criptográficos de la credencial son estáticos y compartidos entre presentaciones.

Anatomía del ataque indirecto

El ciudadano utiliza la misma credencial en dos contextos distintos:

- **RP A** — Sitio de contenido para adultos: solo solicita “mayor de 18 años”.
- **RP B** — Servicio financiero regulado: solicita nombre completo y fecha de nacimiento (KYC).

Ambas presentaciones comparten identificadores únicos y persistentes: firma del emisor, salts y hashes estáticos necesarios para la validación.

Materialización de la amenaza

RP A y RP B comparten con el emisor los elementos únicos recibidos.

El emisor correlaciona ambas transacciones y vincula la actividad anónima con la identidad real del usuario.

El perfil resultante supera lo que cualquiera de las partes conocía por separado, incluida la identidad en el caso de la RP A.

De momento, queda claro que hace falta

01

Credenciales anónimas

Emitir credenciales sin identificadores ni pseudo-identificadores, al menos para los casos de uso en los que se necesita mantener el anonimato.

02

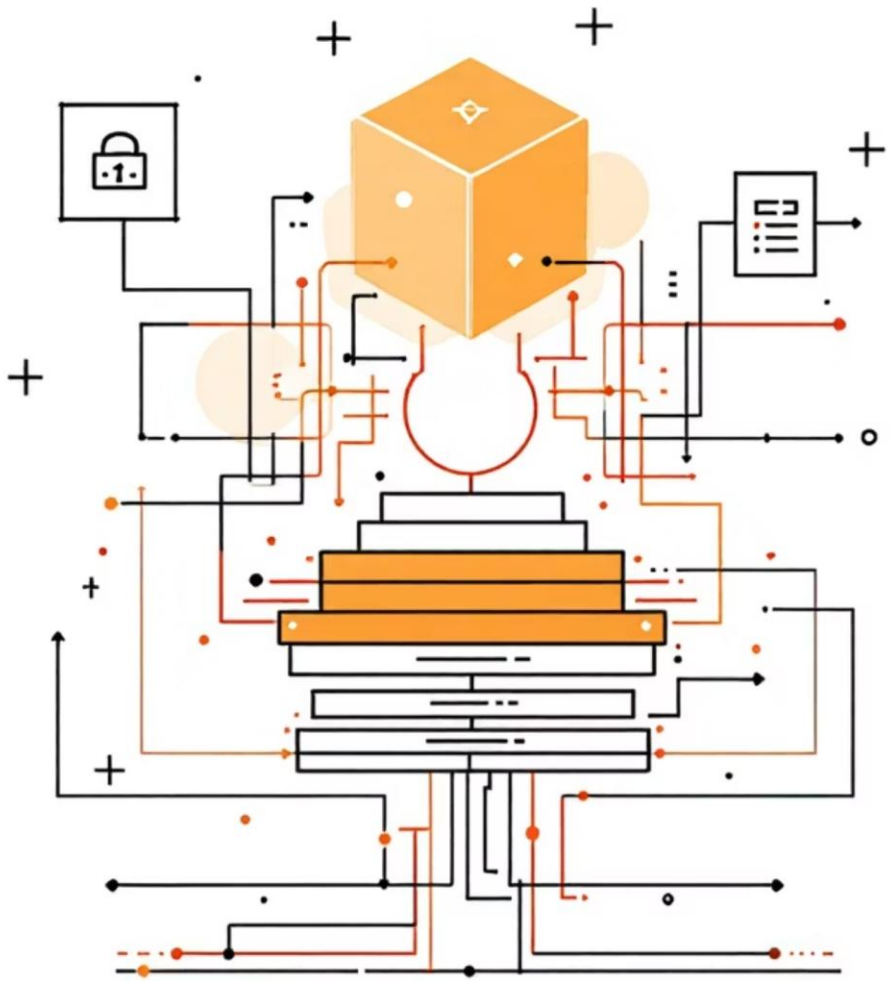
Pruebas de conocimiento cero (ZKP)

Demostrar atributos sin revelar la credencial subyacente (sin presentarla realmente) ni sus elementos criptográficos únicos y vinculables.

03

Certificados de registro

Verificar, de manera automática y escalable, que las RPs registradas cumplen el uso declarado. Auditar incumplimientos y la connivencia entre actores.



4. Otras cosas que podrían salir mal

¿Qué son las amenazas de Inexactitud?

Las amenazas de inexactitud implican el uso de datos obsoletos, erróneos, incompletos, sesgados o de baja calidad que pueden conducir a decisiones incorrectas y causar perjuicios al ciudadano.

Pregunta 1: ¿Es fiable el ecosistema de la cartera? ¿Pueden las partes usuarias (RPs) confiar en mis credenciales para tomar decisiones correctas?

Causas principales de la inexactitud

Credenciales desactualizadas

Los atributos de identidad han cambiado desde la emisión: edad, estatus legal, cualificaciones o condición de revocación.

Errores de software

Fallos en los sistemas que gestionan documentos de identidad pueden introducir inexactitudes durante el procesamiento.

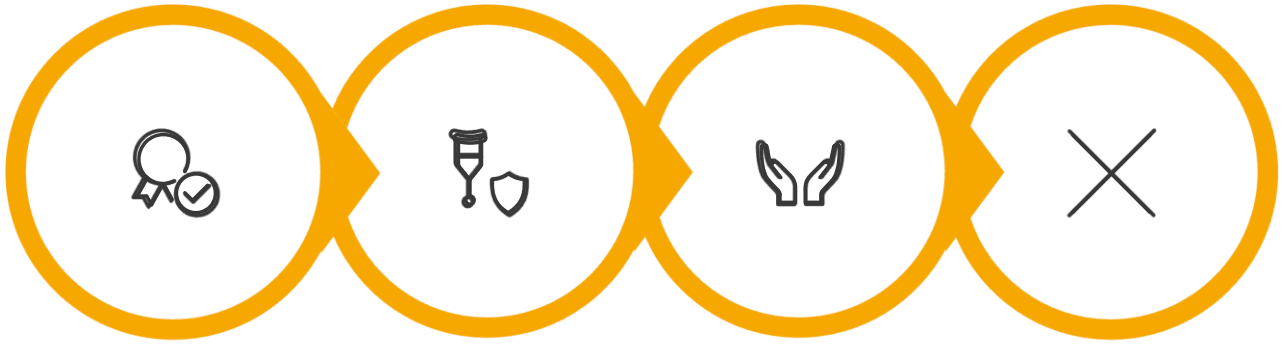
Inconsistencias en verificación

Diferencias de transliteración, homónimos o entradas incompletas en los datos de referencia durante la verificación de identidad.

Ataques

Un adversario compromete los sistemas de verificación para modificar ilegítimamente la información almacenada o manipular el resultado.

Ejemplo: el atributo **age_over_18** obsoleto



Emitida a los 17 años

No actualizada

Presentada a RP

Solicitud denegada

El emisor no revocó ni reemitió la credencial tras el cambio de estatus. La RP toma una decisión incorrecta basada en datos obsoletos y deniega el acceso a un servicio al que el usuario tiene derecho.

Impacto y mitigación de la inexactitud

Impactos principales

Decisiones incorrectas

Comprometen el nivel de garantía de los procesos de verificación de identidad, autenticación y autorización basados en la cartera.

Suplantación de identidad

En escenarios extremos, puede producirse una suplantación de la identidad del ciudadano.

Estrategias de mitigación

1. **Revocación y reemisión**

   Los emisores revocan y reemiten credenciales cuando cambia la información de identidad.

2. **Recordatorios proactivos**

   La cartera alerta al usuario sobre credenciales próximas a caducar o ya caducadas.

3. **Validación en tiempo real por la RP**

   La RP verifica que la credencial no ha sido revocada, no ha caducado ni ha sido reportada como perdida o robada.

¿Qué son las amenazas de No Repudio?

El no repudio impide al interesado negar su participación en una transacción específica en la que se haya utilizado la cartera. En transacciones no legalmente obligadas a conservar registros, se debe garantizar la negación plausible.

? Pregunta 1: ¿Puedo negar haber realizado una transacción que no está legalmente obligada a conservar un registro?

Causas del no repudio

Mecanismos criptográficos vinculables

Las firmas en los formatos ISO mDL y SD-JWT son inherentemente vinculables. La vinculación al dispositivo (WSCD) o por atributos crea registros no repudiables.

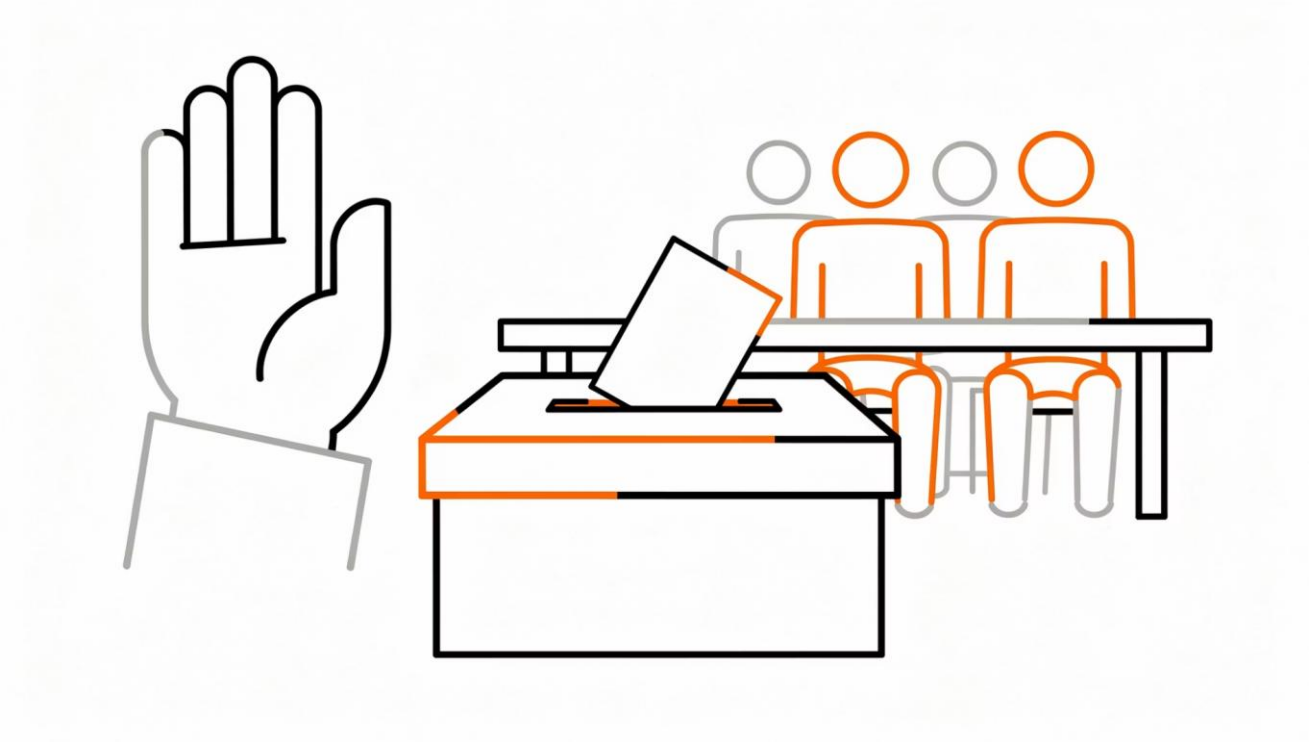
Confabulación entre partes

Emisores, RPs y proveedores de carteras pueden cooperar para correlacionar transacciones y vincularlas de forma persistente al usuario.

Vinculación de credenciales

La presentación combinada de múltiples credenciales vinculadas al mismo WSCD genera una prueba forense de la transacción completa.

Ejemplo: participación en actividades sensibles



Un usuario presenta simultáneamente su credencial de identidad y su credencial de residencia ante una RP para participar en elecciones sindicales, realizar una contribución a una organización de derechos civiles o para acceder a los servicios de una clínica de salud reproductiva.

La cartera genera una firma no repudiable que vincula su dispositivo, los datos combinados y el momento exacto de la transacción.

Importante: Si el contexto político cambia, el usuario puede sufrir el impacto de ser capaza de negar plausiblemente su implicación. El registro permanece.

Impacto y mitigación del no repudio

Impactos principales

Perfilado y vigilancia

Las transacciones vinculables permiten construir perfiles detallados de la actividad del ciudadano a lo largo del tiempo.

Coacción y estigmatización

La existencia de registros no repudiables puede utilizarse para presionar, discriminar o estigmatizar a individuos.

Riesgo para la integridad física

En contextos autoritarios, la imposibilidad de negar puede exponer al ciudadano a consecuencias graves, incluyendo riesgos físicos.

Estrategias de mitigación

1. En general, las ya mencionadas para evitar la vinculación y la identificación

Otras amenazas

Exclusión

¿Qué ocurre si un ciudadano no puede usar la cartera porque no tiene el dispositivo necesario? ¿O los conocimientos necesarios? ¿Y si no quiere usarla, impedirá eso que realice ciertas transacciones?

Detección

¿Se puede detectar que el usuario realiza ciertas transacciones o interactúa con ciertas RP a través de la cartera? ¿Qué ocurre con los logs, por ejemplo?

Falta de capacidad para intervenir

¿Tienen los ciudadanos realmente el control? ¿Pueden tomar decisiones realmente libres e informadas sobre los datos que comparten y con quién? ¿Pueden ejercer todos sus derechos? ¿Habrá situaciones en las que estén sujetos de forma obligatoria a decisiones 100% automatizadas?

5. Conclusiones

Protección de datos desde el diseño y por defecto

No tiene sentido diseñar e implementar carteras que no cumplan con este requisito fundamental, no sólo por cumplimiento, pensemos en los impactos para derechos y libertades.

El momento actual es crítico

Ahora se están tomando decisiones fundamentales sobre la regulación, las especificaciones técnicas, las certificaciones.

La cartera como oportunidad y como amenaza

El nuevo marco europeo ofrece la base regulatoria para construir un ecosistema de identidad digital seguro, respetuoso con la privacidad y verdaderamente europeo. Pero también puede ser una nueva herramienta de vigilancia.

¡GRACIAS!
¿Preguntas?

Dra. Marta Beltrán Pardo
Directora adjunta de Innovación Tecnológica
Subdivisión Científica y de Prospectiva


mbeltran@aepd.es

Fotografías: https://unsplash.com y Wikimedia Commons
Iconos: https://www.flaticon.es/
Diseño: https://gamma.app/